REMARKS

These amendments and remarks are in response to the Office Action dated October 6, 2004. Claims 1-111 are pending in the application.

In the Office Action, the Examiner rejected claims 1, 41, 50, 72, 90 and 108 under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. Further claims 1, 41, 50, 72, 90 and 108 were rejected under 35 U.S.C. § 112, first paragraph, as based on a disclosure which is not enabling. Further claims 1, 41, 50, 72, 90 and 108 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Further claims 1-111 were rejected under 35 U.S.C. § 102(e) as being anticipated by Pat. No. 6,226,642 ("Beranek").

Each of the rejections from the Office Action of October 6, 2004 is discussed below in connection with the various claims. Further, with this response, claim 108 has been amended for clarity and has not been amended for the purpose of patentability. No new matter has been added. Reconsideration of the application is respectfully requested in light of the following amendments and remarks.

I. REJECTIONS UNDER 35 U.S.C. § 112

A. Claim 1, 41, 50, 72, 90 and 108

Claims 1, 41, 50, 72, 90 and 108 were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. Applicant submits that the claims are described in the specification adequately to enable one skilled in the art to make and/or use the invention. For example, the Examiner is referred to paragraphs 117, 126, 142-146 and elsewhere in the Specification.

The Examiner also questions Applicant's use of the descriptors, "first," "second," "third," etc. in reference to the claim term "rules." Applicant submits that these designations are merely descriptors to preserve proper antecedent basis in the claims. However, no specific implementation of the claimed rules is implied and all implementations are contemplated, and accordingly, the way in which the rules are actually implemented is not a claimed limitation. In particular, for example, the claimed first rule may be identical to the second rule, or the first and second rules may be part a larger rule. One of ordinary skill in the art would appreciate that a "rule" is "a prescribed guide for conduct or action." *See* Merriam-Webster's Collegiate Dictionary 1020 (10th ed. 2002). Applicant's use of the term rule is consistent with this definition and is not limited to an HTTP request/response. Instead, the specification's use of the term "rule" is consistent with the above definition. For example:

> Each rule set 726 contains one or more rules 732 which are applied by the packet analyzer to the buffered packet 704. Essentially, each rule 732, described in more detail below, consists of a function and an action to be taken based on the results of the evaluation of the function. The function may involve analysis or examination of one or more portions of the packet 704, and typically comprises a comparison operation which compares one or more portions of the packet 704 with one or more pre-defined values to determine whether or not the associated action should be taken. ... For example, one rule 732 may be to compare the port address from the header data layer 706 to a value of 80 to determine if this is an HTTP packet. Further, the rule set 726 may contain several rules which compare different parts of the packet 704 to different values, in effect creating a compound function. An example would be to determine not only that a particular packet 704 is an HTTP packet but also to then determine the URL contained within the application data layer 708. In addition, a function of a rule 732 may also use the result of another rule 732 in its rule set 726 or another rule set 726 as an input to be evaluated. In addition, state information representing the analysis of past packets may be stored and used by rules 732 to analyze future packets. This functionality, for example, may be used to monitor for sequences of particular packets 704 flowing over the network 100. *See* Specification, para. 142.

> In one embodiment,

> each rule set consist[s] of a hierarchical tree of nodes which are logically linked together, where one or more nodes form a rule. Each tree begins with a root entry node where processing begins. Each node may be one of three types, data gathering, decision or action. Data gathering nodes retrieve data or other information about the current packet, about the current operating environment or about other packets which may be relevant to the current packet being processed and which have been stored for such reference. Data gathering nodes gather information to be used by decision nodes. Decision nodes perform a function utilizing the data gathered by the data gathering nodes such as a comparison function, an equality function, an inequality function, or some other mathematical and/or Boolean operation. An action node uses the result of the decision node to perform some operation on the packet. In the preferred adapter 800, the possible actions include releasing the current packet, copying the current packet and sending the copy to an external device via the external device interface 808, or alternatively, sending the PIB or pointer, deleting the packet or modifying some or all of the packet and releasing it, or combination thereof. Each node specifies another node to

> which processing should continue when processing of the current node is complete. It will be appreciated that the node and tree structure is a logical data organization which may be implemented as a table of pointers or other construct as is known. *See* Specification, para. 159.

Applicant believes that the claims comply with the enablement requirement of 35 U.S.C. § 112, first paragraph. Accordingly, applicants respectfully request the withdrawal of the rejection to these claims.

Claims 1, 41, 50, 72, 90 and 108 were rejected under 35 U.S.C. § 112, second paragraph, as failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically these rejections were made because of the lack of differences between first, second, third, fourth, fifth, and sixth rules along with first and second actions. As explained above, the Examiner's assertion that the claimed rules are HTTP requests/responses is incorrect. Rather the claimed rules are described above. For the reasons stated above, applicants submit that the differences between the first, second, third, fourth, fifth, and sixth rules as well as the first and second actions are adequately described. Accordingly, applicants respectfully request the withdrawal of the rejection to these claims.

II. REJECTIONS UNDER 35 U.S.C. § 102(e)

A. Claim 1, 41, 50, 72, 90 and 108

Claims 1, 41, 50, 72, 90 and 108 were rejected under 35 U.S.C. § 102(e) as being anticipated by Beranek. Applicants submit that claims 1, 41, 50, 72, 90 and 108 are not anticipated by Beranek because Beranek fails to disclose all of the elements of these claims.

Claim 1 is directed to a method of processing a first data packet transmitted over a network from a source to a first recipient, the first data packet comprising a header layer and an application data layer. The method comprises capturing the first data packet from the network prior to its reception by the first recipient. The method further comprises analyzing the header layer of the first data packet according to a first rule. The method further comprises examining, selectively, a dynamically specified portion of the application data layer of the first data packet according to a second rule. The method further comprises determining a first action to be taken on the first data packet according to a third rule. The method further comprises performing the first action on the first data packet.

Claim 41 is directed to a method of processing a first data packet directed to a first recipient over a network, the first data packet comprising header data and application data. The method comprises intercepting the first data packet prior to receipt by the first recipient. The method further comprises capturing the first data packet in a buffer. The method further comprises analyzing, selectively, the header data according to a first rule. The method further comprises analyzing, selectively, a dynamically specified portion of the application data according to a second rule. The method further comprises copying, selectively, the first data packet and forwarding, selectively, the copied first data packet to a second recipient different from the first recipient according to a third rule. The method further comprises releasing, selectively, the first data packet back to said network according to a fourth rule. The method further comprises modifying, selectively, the first data packet and releasing, selectively, the modified first data packet back to said network according to a fifth rule. The method further comprises deleting, selectively, the first data packet from the buffer according to a sixth rule. The method further comprises storing, selectively, information about the first data packet according to a seventh rule.

Claim 50 is directed to an apparatus for processing a first packet transmitted over a network from a source to a first destination, the first packet comprising a header layer and an application data layer. The apparatus comprises a network interface operative to receive the first packet from the source. The apparatus further comprises a routing processor coupled with the network interface and operative to receive the first packet from the network interface and convey the first packet to the first destination. The apparatus comprises a packet processor coupled with the network interface and the routing processor, said packet processor. The packet processor comprises a packet analyzer operative to analyze the header layer according to a first rule and selectively analyze a dynamically specified portion of the application data layer according to a second rule. The packet processor further comprises a packet redirector coupled with the packet analyzer and the routing processor and operative to selectively perform an action on the first packet according to a third rule prior to the conveyance by the routing processor.

Claim 72 is directed to an adapter for a router comprises a router interface operative to couple the adapter with the router. The adapter further comprises a packet processor coupled with the router interface and operative to intercept a first packet prior to receipt by the router. The packet processor comprises a buffer operative to receive and store the first packet for processing. The packet processor further comprises first logic coupled with the buffer, the first logic operative to apply a first function to a header layer of the first packet and produce a first result. The packet processor further comprises second logic coupled with the buffer, the second logic operative to apply a second function to a dynamically specified portion of the application data layer of the first packet and produce a second result. The packet processor further comprises third logic coupled with the buffer and the first and second logic, the third logic operative to perform an operation on the first packet using a third function and the first and second results.

Claim 90 is directed to a system for facilitating a non-invasive interface to a network. The system comprises a router coupled with the network and operative to route a first packet from a first source to a first destination. The system further comprises a packet processor coupled with the router and operative to receive the first packet from the first source and process the first packet prior to routing by the router. The packet processor includes a rule set comprising first, second and third rules. The packet processor further includes first logic operative to analyze a header layer of the first packet according to the first rule. The packet processor further includes second logic operative to analyze a dynamically specified portion of the application data layer of the first packet according to the second rule. The packet processor further includes third logic operative to perform a function on the first packet according to the third rule. The packet processor further includes an external interface operative to transparently couple a first external device to the packet processor.

Amended Claim 108 is directed to an edge server coupled between a point-of-presence ("POP") and a network and operative to monitor a network traffic stream passing between said POP and the network. The edge server comprises a traffic interceptor operative to selectively intercept the network traffic stream between the POP and the network prior to the network traffic stream reaching its intended destination. The edge server further comprises a traffic modifier operative to modify the selectively intercepted traffic and reinsert the modified selectively intercepted traffic into the network.

Beranek discloses a method of controlling how a Web document is presented for display on a browser of a web appliance. *See* Beranek, Abstract. Beranek discloses intercepting and re-formatting a Web document prior to its display on a browser. *See*

Beranek, Col. 2, lines 25-27. The received data stream is intercepted by a proxy which also functions to inject new control information into the data stream in order to affect how the web content is ultimately displayed. *See* Beranek, Col. 13, lines 48-51.

Beranek fails to disclose "capturing said first data packet from said network *prior to its reception* by said first recipient," as claimed in claim 1; "intercepting said first data packet *prior to receipt* by said first recipient," as claimed in claim 41; "a routing processor … operative to receive said first packet from said network interface and *convey* said first packet *to said first destination*," as claimed in claim 50; "a packet processor copupled with said router interface and operative to intercept a first packet *prior to receipt* by said router," as claimed in claim 72; "a packet processor coupled with said router and operative to *receive said first packet* from said first source and process said first packet *prior to routing* by said router," as claimed in claim 90; or "a traffic interceptor operative to selectively intercept said network traffic stream between said POP and said network *prior to said network traffic stream reaching its intended destination*," as claimed in claim 108.

Beranek discloses instead that "[c]onnectivity between the proxy and the browser is achieved using the sockets mechanism by configuring the browser to pass the HTTP requests to the proxy." *See* Beranek, Col. 12, lines 39-42. Further, Beranek states that, "[t]o send an HTTP GET request, the browser creates a packet (including the URL and other information) and then opens a socket using the sockets mechanism. The packet is then sent to an IP address port number to service the HTTP request. Thus, when the browser issues an HTTP GET request, it binds to the socket and sends the request." *See* Beranek, Col. 12, lines 42-47. "The request is then intercepted and processed by the proxy instead of being sent directly over the network, all in the manner previously described." *See* Beranek, Col. 12, lines 47-51.

Beranek, therefore, fails to disclose capturing/intercepting/receiving prior to reception by the intended recipient as claimed in Applicant's claims. In the system disclosed by Beranek, the browser is configured, i.e. directed, to send HTTP GET requests to the proxy. Effectively then, the proxy is not intercepting the requests because it is the intended recipient/destination of the requests made by the browser. The proxy receives those requests, which were directed to it by the browser, and, therefore, the proxy is not intercepting these requests prior to their receipt, as claimed. Therefore, Beranek fails to disclose intercepting the first data packet prior to its reception as claimed.

For at least the reasons stated above, Beranek does not disclose all of the elements in claims 1, 41, 50, 72, 90 and 108. Accordingly applicants respectfully request the withdrawal of the rejection to claims 1, 41, 50, 72, 90 and 108 under 35 U.S.C. § 102(e).

B. Dependent Claims 2-40, 42-49, 51-71, 73-89, 91-107 and 109-111

Dependent claims 2-40, 42-49, 51-71, 73-89, 91-107 and 109-111 were also rejected under 35 U.S.C. § 102(e) as being anticipated by Beranek. Claims 2-40 are dependent on independent claim 1, claims 42-49 are dependent on independent claim 41, claims 51-71 are dependent on independent claim 50, claims 73-89 are dependent on independent claim 72, claims 91-107 are dependent on independent claim 90, and claims 109-111 are dependent on independent claim 108. As explained above, Beranek does not disclose all of the elements of independent claim 1, 41, 50, 72, 90 or 108. Accordingly, Beranek does not disclose all of the elements of claims 2-40, 42-49, 51-71, 73-89, 91-107 and 109-111 which depend from the independent claims. Therefore, Applicants respectfully request the withdrawal of the rejection to claims 2-40, 42-49, 51-71, 73-89, 91-107 and 109-111 under 35 U.S.C. § 102(e).

CONCLUSION

In view of the foregoing remarks and amendments, Applicants submit that the pending claims are in condition for allowance. Reconsideration is therefore respectfully requested. If there are any questions concerning this response, the Examiner is asked to phone the undersigned attorney at (312)-321-4200.

Respectfully submitted,

Dated: December 28, 2004

James L. Katz
Registration No. 42,711
Attorney for Applicants

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200